Greater Manchester Shared Services

GMSS
Secure Transfer Policy

Review Date: October 2019

Programme:	Greater Manchester Shared Services
Filename:	I:\GMSS\GDPR\POLICIES
Author:	GMSS IG Team
Version:	1.2
Date Released:	April 2017
Purpose of this document:	This documents outlines GMSS Secure Transfer Policy

Document Location

Copies of this document can be obtained from|:

Name:	Corporate Services Office
Address:	Greater Manchester Shared Services Ellen House Waddington Street Oldham OL9 6EE
Telephone:	0161 212 4186

Revision History

Revision date	Revision by	Summary of changes	Version
November 2016	GMSS IG Team	Reviewed from Oldham CCG to fit GMSS	0.1
November 2016	GMSS IG Group	Recommend approval by the IG Group	0.1
January 2017	FPG	Recommend approval after some amendments	0.1
January 2017	SMT	Amendments needed	0.1
August 2017	GMSS IG Team	Changed to accommodate GDPR	1.1

Approvals

Name	Role	Date	Version
SMT		February 2017	1.0
IG Group		18th October 2017	1.2

DOCUMENT STATUS:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

Contents

1. Introduction

The purpose of this policy is to provide guidance to all Greater Manchester Shared Services (hereafter referred to as 'GMSS') staff on the secure transfer of information.

A number of Acts and guidance dictate the need for secure transfer arrangements to be set in place; they include (but are not restricted to):

Data Protection Act

The new **General Data Protection Regulation** (namely article 5): "Appropriate technical and organisational measures shall be taken to make personal data secure"

NHS Code of Practice: Confidentiality (namely Annex A1 Protect patient Information) "Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be"

GMSS staff must maintain the confidentiality of personal confidential data when both using it and transmitting data.

Where the term Safe Haven is used, it refers to a location (or in some cases a piece of equipment such as a fax machine) situated on GMSS premises where arrangements and procedures are in place to ensure sensitive or confidential information can be held, received and communicated securely.

Depending on the content of information being sent the Secure Transfer policy should be applied when it is of a Personal/Sensitive/Confidential nature.

When information is being transferred from one GMSS/location/organisation to another, staff need to be confident of the safety and security of how the information is being transmitted.

This document sets out a framework within which staff responsible for all routine flows of personal confidential data, personal staff information and commercial in confidence information and any similar exchanges should adhere to. Any data flow must be between designated safe haven contact points. NHS staff use a wide variety of methods of handling and transferring confidential Information. List below:

- Fax Machines
- Answer Phones
- Telephones
- Photocopiers
- Email
- Message Books
- Post
- Visitors Books
- Dictation Machines
- Removable Media
- Bulk Data Transfers

This guidance is designed to protect GMSS as an organisation, its constituent businesses and staff by defining the use and application of encryption technology when accessing, storing and transmitting GMSS corporate, personal or patient information.

2. GMSS Scope

This guidance applies to those members of staff who are directly employed by GMSS and for whom GMSS has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of GMSS. This policy also applies to all third parties and others authorised to undertake work on behalf of GMSS.

This guidance relates specifically to the handling of personal confidential data both clinical and non-clinical that has been received, created, maintained, stored or destroyed by staff by GMSS (refer to Paragraph 1).

This guidance aims to raise awareness and provide guidance on: The legislation and guidance which dictates the need for a safe haven

A definition of the term safe haven when a safe haven is required

The necessary procedures and requirements that are needed to implement a safe haven environment.

3. Definitions

Person Identifiable information, now known as Personal Confidential Data (PCD)

Personal Confidential Information (PCD) is information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Sensitive Personal Information

Sensitive personal information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community, for example, where the personal information contains details of the individual's:

- Health of physical condition Sexual life
- Ethnic origin
- Religious beliefs Trade union
- Political opinions
- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that data remains secure.

Business Sensitive information

This is information that if disclosed could harm or damage the reputation or image of an organisation.

Safe Haven

The term safe haven is term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure personal confidential data is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

bogus
This term was initially meant to describe the transfer of fax messages but is now covered in the data held and used within

- Fax machines
- Telephones/answer phones Photocopiers
- Emails
- White boards/notice boards Manual records and books
- Dictation Machines Removable Media Bulk data transfers

4. Accountability, Responsibilities and Training

Managing Director
The Managing Director has overall responsibility for Information Governance within GMSS. As Accountable Officer, they are responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner (SIRO) is responsible for identifying and managing the information risks to GMSS. This includes oversight of the organisation's information security / governance incident reporting and response arrangements and the Registration Authority business process. The Deputy SIRO supports the work of the SIRO

Caldicott Guardian
The Caldicott Guardian is a senior person responsible for protecting the confidentiality of the patient and service user information and enabling appropriate information sharing. The Deputy Caldicott Guardian supports this work.

Associate Directors
Line Managers
Information Asset Owners
Have responsibility for ensuring that all staff are aware of the Secure Transfer of Information Policy and to report any new flows in or out of the department/team/service/location or installation of communication modes such as a new fax machine to the GMSS Information Governance Team.

All staff have a responsibility for ensuring the information is handled, used, stored and shared confidentially and appropriately. If in doubt individuals should seek guidance from their line manager in the first instance, or GMSS Information Governance Team.

Staff will receive instruction and direction on this guidance from a number of sources.

- Policy/strategy and procedure manuals Line Manager

- Specific Training Course
- Other communication methods (Staff Briefing, Team Meetings)

5. Best Practice Location/Security Arrangements - Secure Transfer Environment

The Secure Transfer of Information Policy should be in place in any location where confidential data is being received held or communicated especially where the data is person identifiable.

When choosing a safe haven location the follow factors must be considered:

- A safe haven location must be a room that is locked or accessible via a coded key pad (or similar device) known only to authorised staff
- The office or workspace must be sited in such a way that only authorised staff can enter that location
- If sited on the ground floor any windows must have locks on them
- The room must conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage

Manual paper records containing personal confidential data must be stored in locked cabinets when not in use and when the office/workstation is left unattended.

Operate a Clear Desk Policy, e.g. lock documents away if away from desk during the day, evenings and weekends.

Documents should not be left unattended for any significant period of time e.g. faxes should be collected/distributed from the fax machine at frequent periods and post should not be left unattended in pigeon holes or desks.

Computers must not be left on view or accessible to unauthorised staff and must have a secure screen saver function and be switched off when not in use. All staff must 'Lock' their screens when away from desk.

Equipment such as fax machines in the safe haven must have a code password or pin and be turned off out of office hours.

6. Data Transmission Processes

Transmission of Personal Information via Computer and Email

Access to any PC must be password protected and passwords must **not** be shared

Computer screens must not be left on view so that members of the general public or staff who do not have a justified need to view the information can see personal data. PCs or laptops not in use should be switched off or have a secure screen saver device in use.

Information must be held on the organisation's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures

The only accredited and secure way of transmitting patient-identifiable data by e-mail is via NHS Mail between NHS Mail accounts for NHS users. As long as both sender and recipient have the suffix @nhs.net, i.e. (firstname.secondname@nhs.net) emails will be sent/received via encrypted mail service.

Non NHS domains for secure encrypted email transmission can be sent to and from Nhs.net to one of the following:

- .x.gsi.gov.uk
- .gsi.gov.uk
- .gse.gov.uk
- .gsx.gov.uk
- .police.uk
- .pnn.police.uk
- .cjsm.net
- .scn.gov.uk
- .gcsx.gov.uk

To maintain confidentiality of data, outside third party organisations that do not have NHS Mail should have approved encryption software (AES) and a password has to be set which must consist of 8 characters long with a combination of numbers and letters. The password should be supplied by telephone to the recipient, and not issued in a separate email. Alternatively, documents emailed to GMSS may be password protected.

All emails issued by GMSS staff should include the standard disclaimer notice. Personal information of a more sensitive nature must be sent over NHS Mail with appropriate safeguards:

- Emails which contain sensitive information should be appropriately titled i.e. do not include sensitive details in the subject line
- Clinical information is clearly marked
- E-mails are sent to the right people
- Browsers are safely set up so that, for example, passwords are not saved and temporary internet files are deleted on exit
- The receiver is ready to handle the information in the right way

Information Disclosure of Information by Telephone

There will be occasions when telephone enquiries are received asking for disclosure of personal information. When the disclosure is legally justified and the caller has a legal right to access that information, the following rules should be adhered to:

- Verify personal details
- Obtain and record enquiries, telephone numbers etc..
- If the caller is part of an organisation/company, the main switchboard number of that organisation (via phone book or directory enquiries) should be obtained and ring back
- Conduct the call in area that is private where staff/public cannot overhear
- Any notes made during the calls should be kept in a secure place (locked away) and not left on any desk
- Any suspect bogus enquiries should be referred immediately to the GMSS Information Governance Team as soon as possible and an incident form completed
- Always provide the minimum amount of information that is necessary
- If in doubt, the caller should be advised that they will be called back, where necessary, a senior manager or the designated authority for confidentiality issues should be consulted
- Be aware of any press enquiries and refer to the relevant department within GMSS

Communications by Post

Incoming:

- Ensure incoming post is received in an environment away from public interference e.g. not left on receptionist's desk in a waiting area
- Open incoming mail away from public areas
- Ensure if post is sorted for onward distribution that it is stored securely and is picked up frequently

Outgoing:

- Always double check addresses
- Mark post clearly with names and addresses and with 'Private and Confidential'
- Use a GMSS letter headed front page or compliment slip
- Use a secure robust envelope, include a return address where appropriate
- For important letters/parcels, ask for confirmation of safe arrival
- Outgoing sensitive information should be protected from data loss in line with Department of Health guidance, by using a trackable service, i.e. Royal Mail Special Delivery or GMSS's authorised courier. Royal Mail Recorded Delivery is not a trackable service.

Communications by Text Message

Text messaging is becoming increasingly popular however there are potential information security risks that should be considered before any text messages are used. For example:

- Check the mobile number is correct and be confident that the person using the recipients mobile is the person to whom the message is intended
- Check that the patient has received the message
- Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) – as mobile phones are easy to misplace or may get stolen there is a danger of a breach of confidentiality occurring that the patient may find embarrassing or damaging
- Mobile phone networks may be open to additional risks of eaves dropping or interception

When using this method of communication minimum amount of confidential data should be sent. And remember that appropriate informed consent must have been sought prior to commencing text messaging communications.

Transfer of Paper/Hardcopy Documents

Paper records/documents may be required for investigation or to refer to as part of patients care. Care must be taken when transferring documents that contain confidential information:

- Paper documents that contain confidential information must be stored in a lockable cupboard or cabinet
- Lockable crates must be used to move bulk hardcopy information
- Only take off site when absolutely necessary, or in accordance with local policy Record what information is taken off site/from a department, and if applicable,
- where and whom the information has gone to
- Ensure documents are properly 'booked out' of any relevant filing

- Never leave personal/sensitive/confidential records/documents unattended Ensure the information is returned as soon as possible
- Record that the information has been returned

For further information on transferring paper documentation please refer to GMSS Records Management Policy

Other Electronic Media

- Dictation machines and tapes can contain extremely sensitive information and should always be kept in a locked area when not in use. They should be cleared of all dictation when the communication has been completed
- Answer phones receiving personal information must have the volume lowered so that the information is not being un-necessarily overheard
- Photocopying machines should be sited in areas where the general public do not have physical access. No papers should be left on the glass after copying, *Always Check*.

7. Sharing information with non NHS organisations

Staff should be aware of the Data Sharing Processor Agreement and the requirement to have an Information Sharing Agreement in place for the routine sharing of personal confidential data.

Staff authorised to share/disclose personal information to other organisations outside the NHS must seek assurance that these organisations have a designated safe haven point for receiving personal confidential data

GMSS must be assured that these organisations are able to comply with the secure transfer ethos and that they meet certain legislative and related guidance:

- Data Protection Act
- General Data Protection Regulation
- Common law duty of confidence
- NHS Code of Practice: Confidentiality

8. Monitoring and review

Performance against Service Delivery Measures will be reviewed on an annual basis and used to inform the development of future procedural documents.

This policy will be reviewed on a two yearly basis and in accordance with the following as and when required:

- Legislative changes
- Good practice guidance; case law
- Significant incidents; reported new vulnerabilities
- Changes to GMSS organisations structure

9. Legislation and IG Related Documents

This policy and a set of procedural document manuals are available in GMSS folders.

A number of other policies are related to this policy and all employees should be aware of the full range below:

- Information Governance Framework
- Information Governance Policy
- Data Protection and Confidentiality Policy
- Corporate Information Security Policy
- Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- Information Governance & Cyber Security Incident Reporting Policy
- Encryption Policy
- Confidentiality Audit Policy
- Information Security Policy

Acts Covered Under Policy

- General Data Protection Regulation
- Data Protection Act

.